Catalyst 2960/2950 Series Switches Using Voice VLAN Configuration Example

Document ID: 113260

Contents

Introduction

This document provides a sample configuration for voice VLAN on Cisco Catalyst 2960/2950 Series Switches. Specifically, this document shows how to configure the voice VLAN feature on a Cisco Catalyst 2950 Switch.

Prerequisites

Requirements

Make sure that you meet these requirements before you attempt this configuration:

- Have a basic knowledge of configuration on Cisco Catalyst 2960/2950 Series Switches.
- Have a basic understanding of voice VLAN.

Components Used

The information in this document is based on the Cisco Catalyst 2950 Switch.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Voice VLAN Overview

The voice VLAN feature permits the switch ports to carry voice traffic with Layer 3 IP precedence and Layer 2 class of service (CoS) values from an IP phone. Based on **IEEE 802.1p CoS**, the switch supports quality of service (QoS) which uses classification and scheduling to send network traffic from the switch. You can configure the Cisco IP phone to forward traffic with an IEEE 802.1p priority, and configure the switch to trust or override the traffic priority assigned by an IP phone.

You can configure the switch port, which is connected with an IP phone, to use one VLAN for voice traffic and another VLAN for data traffic from a device attached to the access port of the IP phone. You can configure access ports on the switch to send **Cisco Discovery Protocol (CDP)** packets in order to instruct an attached IP phone to send voice traffic to the switch by any of these methods:

- In the voice VLAN tagged with a Layer 2 CoS priority value
- In the access VLAN tagged with a Layer 2 CoS priority value
- In the access VLAN, untagged (no Layer 2 CoS priority value)

The switch can process data traffic which comes from the device attached to the access port on the IP phone. You can configure the switch ports which send CDP packets that instruct the attached IP phone to configure the mode (trusted or untrusted mode) for the access port on the phone.

In **trusted mode**, the access port on the IP phone passes the traffic from the PC without any change. In **untrusted mode**, the access port on the IP phone receives all traffic in IEEE 802.1Q frames which contain a configured Layer 2 CoS value. The default Layer 2 CoS value is 0. Untrusted mode is the default.

Configure

In this section, you are presented with the information to configure the voice VLAN features described in this document.

In the switch, the voice VLAN feature is disabled by default. When you enable the voice VLAN on the port, all untagged traffic is sent according to default CoS priority. Before you enable voice VLAN, enable the QoS on the switch by issuing the **mls qos** global configuration command and configure the port's trust state to **trust** by issuing the **mls qos trust cos** interface configuration command.

By default, a switch port drops any tagged frames in hardware. In order to accept tagged frames on a switch port, one of these commands should be configured on the port:

- **switchport voice vlan dot1p**
- **switchport voice vlan** *V_VLAN_ID*
- **switchport mode trunk**

Use the **switchport voice vlan dot1p** command in order to instruct the switch port to use the IEEE 802.1p priority tagging to forward all voice traffic with a higher priority through the native (access) VLAN.

Use the **switchport voice vlan** *V_VLAN_ID* command in order to configure a specified voice VLAN, so the IP phone can send voice traffic in IEEE 802.1Q frames with a Layer 2 CoS value. The Cisco IP phone can also send untagged voice traffic or it can use its own configuration to send voice traffic to the access VLAN of the switch.

Use the **switchport priority extend trust** command in order to extend the trust state to the device (PC) connected to the IP phone. By issuing this command, the switch will instruct the phone on how to process the data packets from the device attached to the access port on the Cisco IP phone. Packets generated by the PC

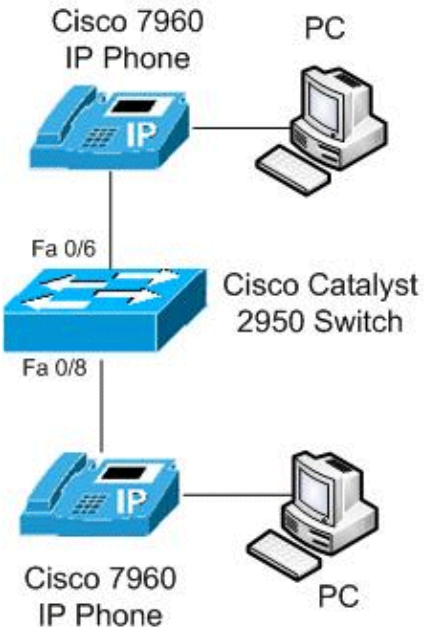
use an assigned CoS value in the 802.1q header. The phone should not change (trust) the priority of frames arriving on the phone port from PC.

You must enable the **CDP** on the switch port to which the IP phone is connected. By default, the CDP is enabled globally on the switch interfaces. CDP is the mechanism used between the switch and Cisco IP phone in order to configure the Cisco IP phone for communication with the switch port. CDP is proprietary to Cisco Systems and other manufacturers phones may not be able to use this method to configure the IP phone to match the switch s port configuration.

Note: Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

Network Diagram

This document uses this network setup:



This diagram is an example of a voice VLAN configuration on a Cisco Catalyst 2950 Switch. The switch ports FastEthernet 0/6 and 0/8 are connected with a Cisco IP phone, and the access port on both the IP phones is connected to the PC.

Configurations

This document uses these configurations:

Based on Trusted CoS Value

In the 2950 switch, the FastEthernet 0/6 port has configured **VLAN 10** for voice VLAN with **dot1p** to use **IEEE 802.1p** priority tagging for voice traffic, and configured **trust** mode for data traffic from the PC which is connected to the access port of the Cisco IP phone. Here, the Cisco IP phone is **trusting** a laptop or PC via CoS and data traffic uses **native VLAN**. This configuration is typically used for management workstations, high−priority users, or a high CoS value application.

When a Cisco phone does CDP with the switch, the trust boundary is always extended to the IP phone. That is, the IP phone's packets are never changed from CoS 5 to CoS default. That is why the **switchport priority**

extend trust command is used for the laptop or PC. It is sent via CDP to tell the IP phone not to rewrite high−priority packets.

The FastEthernet 0/8 port is configured with separate VLANs for voice and data traffic. In this example, **VLAN 10** is used for voice traffic and **VLAN 20** is used for data traffic. This configuration is used for typical Cisco IP phones **without trusting** the laptop or PC. Traffic uses the IEEE 802.1Q frame type.

With the **mls qos trust cos** command, the Catalyst switch's port looks at the CoS value on the Ethernet header for classifying ingress traffic and trusts the tagged packet's CoS value originating from the Cisco IP phone. By default, the Ethernet port becomes untrusted, so the traffic coming from the voice VLAN and the data VLAN will not be trusted.

Use the **priority−queue out** command in order to give voice packets head−of−line privileges when trying to exit port preventing jitter. The **spanning tree portfast** command removes the interface from the spanning tree protocol, and the **bpduguard** command protects the network should someone try to connect a new switch to it after unplugging the IP phone. If a switch were to be plugged in, the port would go to err−disable. These are typically added to phone ports.

Cisco Catalyst 2950 Switch

```
Switch#configure terminal
Switch(config)#mls qos
Switch(config)#interface fastethernet 0/6


!--- Set the interface to classify incoming traffic packets by
 using the packet CoS value.

Switch(config-if)#mls qos trust cos


!--- Configure the phone to use IEEE 802.1p priority tagging for
 voice traffic.

Switch(config-if)#switchport voice vlan dot1p
Switch(config-if)#switchport voice vlan 10


!--- Trust the CoS value the PC sends in on the data VLAN.

Switch(config-if)#switchport priority extend trust
Switch(config-if)#priority-queue out
Switch(config-if)#spanning-tree portfast
Switch(config-if)#spanning-tree bpduguard enable
Switch(config-if)#exit


Switch(config)#interface gigabitethernet0/8
Switch(config-if)#mls qos trust cos


!--- Configure specified VLANs for voice and data traffic.

Switch(config-if)#switchport voice vlan 10
Switch(config-if)#switchport access vlan 20

Switch(config-if)#priority-queue out
Switch(config-if)#spanning-tree portfast
Switch(config-if)#spanning-tree bpduguard enable
Switch(config-if)#exit
```

When Using a Non−Cisco IP Phone

If you are using a non−Cisco IP phone that does not recognize the Cisco proprietary CDP and automatically sets up the trunk port, you will have to configure the trunk manually. In this configuration example, we restrict the VLANs to 10 and 20, and block the default native VLAN 1 or VLAN 0. **VLAN 10** is used for voice traffic and **VLAN 20** is used for data traffic. The non−Cisco IP phone learns the correct VLAN for its tagged packets through manual configuration or via the TFTP file it downloads during boot up. This example uses this configuration:

Cisco Catalyst 2950 Switch

```
Switch#configure terminal
Switch(config)#interface fastethernet 0/6


!−−−Trusts tagged packets CoS value; all untagged packets reset DSCP
value in IP header to 0.

Switch(config−if)#mls qos trust cos


!−−− Turn off DTP (dynamic trunking protocol).

Switch(config−if)#switchport nonegotiate


!−−− Forces the port into trunking mode.

Switch(config−if)#switchport mode trunk
Switch(config−if)#switchport trunk native vlan 20


!−−− Restricts the VLANs.

Switch(config−if)#switchport trunk allowed vlans 10,20
Switch(config−if)#priority−queue out
Switch(config−if)#spanning−tree portfast trunk
Switch(config−if)#spanning−tree bpduguard enable
Switch(config−if)#exit
```

Based on Trusted DSCP Value in IP Header

Here, we use a trusted DiffService Code Points (DSCP) value instead of a CoS value, because CoS offers a way to understand the importance of the packet just by looking at its L2 header. DSCP is a 6−bit field within the IP packet. Use the **mls qos trust DSCP** command in order to trust the DSCP value in the IP header. In this case, the IP phone sets its DSCP correctly in its packets and the laptop would set its DSCP correctly. This example uses this configuration:

Cisco Catalyst 2950 Switch

```
Switch#configure terminal
Switch(config)#interface fastethernet 0/6


!−−−Trust the DSCP value in the IP header.

Switch(config−if)#mls qos trust DSCP


!−−− IP phone VLAN
```

```
Switch(config-if)#switchport voice vlan 10
Switch(config-if)#switchport access vlan 20


!--- Trust the DSCP value the PC sends in on the data VLAN.

Switch(config-if)#switchport priority extend trust
Switch(config-if)#priority-queue out
Switch(config-if)#spanning-tree portfast
Switch(config-if)#spanning-tree bpduguard enable
Switch(config-if)#exit
```

Verify

Use this section to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

- Use the **show interfaces** *interface-id* **switchport** command in order to verify your voice VLAN configuration.

  For example:

  ```
  Switch#show interfaces FastEthernet 0/6 switchport
  Name: Fa0/6
  Switchport: Enabled
  Administrative Mode: dynamic desirable
  Operational Mode: static access
  Administrative Trunking Encapsulation: dot1q
  Operational Trunking Encapsulation: native
  Negotiation of Trunking: On
  Access Mode VLAN: 1 (default)
  Trunking Native Mode VLAN: 1 (default)
  Voice VLAN: dot1p
  Administrative private-vlan host-association: none
  Administrative private-vlan mapping: none
  Administrative private-vlan trunk native VLAN: none
  Administrative private-vlan trunk encapsulation: dot1q
  Administrative private-vlan trunk normal VLANs: none
  Administrative private-vlan trunk private VLANs: none
  Operational private-vlan: none
  Trunking VLANs Enabled: ALL
  Pruning VLANs Enabled: 2-1001
  Capture Mode Disabled
  Capture VLANs Allowed: ALL
  Protected: false
  Unknown unicast blocked: disabled
  Unknown multicast blocked: disabled
  Appliance trust: trusted
  ```
- Use the **show running-config interface** *interface-id* command in order to verify your voice VLAN entries for a particular interface.

  For example:

  ```
  Switch#show running-config interface fastEthernet 0/6
  Building configuration...

  Current configuration : 139 bytes
  !
  interface FastEthernet0/6
  ```

```
 switchport voice vlan dot1p
 switchport voice vlan 10
 switchport priority extend trust
 mls qos trust cos
 priority-queue out
 spanning-tree portfast
 spanning-tree bpduguard enable
end

Switch#show running-config interface fastEthernet 0/8
Building configuration...

Current configuration : 137 bytes
!
interface FastEthernet0/8
 switchport voice vlan 10
 switchport access vlan 20
 mls qos trust cos
 priority-queue out
 spanning-tree portfast
 spanning-tree bpduguard enable
end
```

Related Information

- **Cisco Catalyst 2950 Series Switches Support Page**
- **Cisco Catalyst 2960 Series Switches Support Page**
- **Switches Product Support**
- **LAN Switching Technology Support**
- **Technical Support & Documentation − Cisco Systems**

Updated: Oct 04, 2011 Document ID: 113260
